JOURNAL OF NUMBER THEORY 4, 408–410 (1972)

Binary Quadratic Forms of Determinant $-pq$

EZRA BROWN

Department of Mathematics, Virginia Polytechnic Institute and State University, Blacksburg, Virginia 24061

Communicated by O. Taussky Todd

Received July 17, 1970

The following theorem is proved: If p and q are distinct primes of the form $4n + 1$, and $(p \mid q) = 1$, then $x^2 - pqy^2$ represents -1 if $(p \mid q)_4 = (q \mid p)_4 = -1$; p if $(q \mid p)_4 = -(p \mid q)_4 = 1$; q if $(p \mid q)_4 = -(q \mid p)_4 = 1$. If $(p \mid q)_4 = (q \mid p)_4 = 1$, there are examples with any of the three being represented.

If p and q are distinct primes of the form $4n + 1$, then $x^2 - pqy^2$ represents one and only one of -1, p, and q [3]. If $(p \mid q) = -1$, then -1 is represented, but if $(p \mid q) = 1$, both ambiguous classes lie in the principal genus. We shall prove:

THEOREM. *If p and q are distinct primes of the form $4n + 1$, and $(p \mid q) = 1$, then $x^2 - pqy^2$ represents -1 if $(p \mid q)_4 = (q \mid p)_4 = -1$; p if $(q \mid p)_4 = -(p \mid q)_4 = 1$; q if $(p \mid q)_4 = -(q \mid p)_4 = 1$. If $(q \mid p)_4 = (p \mid q)_4 = 1$, there are examples with any of the three being represented.*

In this article, if $(p \mid q) = 1$, we write $(p \mid q)_4 = 1$ or -1 to indicate that p is or is not a fourth-power residue of q. We make use of the following interesting result, due to K. Burde (see [1]):

LEMMA 1. *If $p = a^2 + b^2$, $q = c^2 + d^2$, $a \equiv c \equiv 1$, $b \equiv d \equiv 0 \pmod 2$, $ab > 0$, $cd > 0$, p and q are primes, and $(p \mid q) = 1$, then*

$$(p \mid q)_4 (q \mid p)_4 = (-1)^{(p-1)/4} (ad - bc \mid p).$$

LEMMA 2. *If $x^2 - pqy^2$ represents p, then $(q \mid p)_4 = 1$; if $x^2 - pqy^2$ represents q, then $(p \mid q)_4 = 1$.*

Proof. Suppose $t^2 - pqu^2 = p$; then t is odd, u is even, and $[pqu/2, t, u/2]$ is a form of discriminant p, so that $((u/2) \mid p) = 1$. Writing

$t = mp$, we have $m^2p - qu^2 = 1$, so that $qu^2 \equiv -1 \pmod{p}$. Hence $(q \mid p)_4 = (-4(u/2)^2 \mid p)_4 = (-1 \mid p)_4 (2 \mid p)((u/2) \mid p) = 1$, since if p is of the form $4n + 1$, then $(-1 \mid p)_4 = (2 \mid p)$. Analogously, if $x^2 - pqy^2$ represents q, then $(p \mid q)_4 = 1$.

LEMMA 3. *If $x^2 - pqy^2$ represents -1 and $(p \mid q) = 1$, then there exist integers a, b, c, and d such that $p = a^2 + b^2$, $q = c^2 + d^2$, $a \equiv c \equiv 1$, $b \equiv d \equiv 0 \pmod{2}$, $ab > 0$, $cd > 0$, and $(ad - bc \mid p) = (2 \mid p)$.*

Proof. Suppose $t^2 - pqu^2 = -1$. The form $[pqu, 2t, u]$ has determinant 1, so by a result of Cantor [2], the class of $[1, 0, -pq]$ contains a form $[r, 2s, -r]$. This class primitively represents $2s$, so $(2s \mid p) = 1$, $pq = r^2 + s^2$, r is odd, and s is even. Writing $p = a^2 + b^2$, $q = c^2 + d^2$, where $a \equiv c \equiv 1$, $b \equiv d \equiv 0 \pmod{2}$, we have, for some suitable choice of sign, $(2 \mid p) = (s \mid p) = (ad \pm bc \mid p)$. But $(ad - bc)(ad + bc) = pd^2 - b^2(c^2 + d^2) \equiv -b^2q \pmod{p}$, and $(q \mid p) = 1$, so that $(ad - bc \mid p) = (ad + bc \mid p)$. Hence we may choose $ab > 0$ and $cd > 0$, and our conclusion follows.

LEMMA 4. *If $x^2 - pqy^2$ represents -1, then $(p \mid q)_4 = (q \mid p)_4$.*

Proof. If $x^2 - pqy^2$ represents -1, then by Lemma 3, there exist integers a, b, c, and d such that $p = a^2 + b^2$, $q = c^2 + d^2$, $a \equiv c \equiv 1$, $b \equiv d \equiv 0 \pmod{2}$, $ab > 0$, $cd > 0$, and $(ad - bc \mid p) = (2 \mid p)$. By Lemma 1, we then have $(p \mid q)_4 (q \mid p)_4 = (-1)^{(p-1)/4} (2 \mid p)$, which is easily seen to be 1 for p of the form $4n + 1$. The desired conclusion follows from this.

Proof of the Theorem. By Lemma 4, if $x^2 - pqy^2$ represents -1, then $(p \mid q)_4 = (q \mid p)_4$. By Lemma 2, if q is represented, $(p \mid q)_4 = 1$, and if p is represented, $(q \mid p)_4 = 1$. The first sentence of the theorem is immediate from these statements and from the fact that one and only one of $-1, p$, and q is represented. As for the last sentence, $(p \mid 5)_4 = (5 \mid p)_4 = 1$ for $p = 101$, 181, and 461; however, $x^2 - 5py^2$ represents 5, 181, and -1, respectively.

The conditions of representation of p (or q) appear in the body of an article by A. Scholz [4], not in the title. He uses class field theory methods.

REFERENCES

1. K. BURDE, Ein rationales biquadratisches Reziprozitätsgesetz, *J. Reine Angew. Math.* **235** (1969), 175–184.

2. G. CANTOR, Zwei Sätze aus der Theorie der binären quadratischen Formen, *Z. Math. Phys.* **13** (1868), 259–261.
3. G. PALL, Discriminantal divisors of binary quadratic forms, *J. Number Theory* **1** (1969), 525–533.
4. A. SCHOLZ, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, *Math. Z.* **39** (1935), 95–111.